SYSTEM AND METHOD FOR SELECTIVE ENHANCED DATA CONNECTIONS IN AN ASYMMETRICALLY ROUTED NETWORK

FIELD OF THE INVENTION

[0001]   The invention relates to the field of communications, and more particularly to platforms and techniques for establishing enhanced dial-up connections to the Internet or other networks, such as connections having added compression, caching, optimization, and security or other services.

BACKGROUND OF THE INVENTION

[0002]   While broadband technologies such as cable modem, digital subscriber line (DSL) and others have enjoyed market growth, a significant proportion of consumers still rely upon dial-up connections over the public switched telephone network (PSTN) to access the Internet and other networks. Dial-up modem connections retain the advantages of low cost, standardized hardware and protocols, near-universal accessibility and throughput that remains sufficient for many desired services, including email, instant messaging and others.

[0003]   Commercial Internet Service Providers (ISPs) and others have therefore continued to solicit and provision dial-up users. The provisioning of dial-up service may involve deploying dial-up paths which direct the user's incoming modem call to the provider via a dedicated point-to-point protocol (PPP) connection. As illustrated in Fig. 1, this may conventionally involve receiving incoming calls over the PSTN via the local switch of a local exchange carrier or other telephone service provider. The dial-up modem call may be received in a modem bank, remote access server (RSA) or other terminal equipment which synchronizes with the consumer's modem while password, username or other information is authenticated.

1

[0004]   Once connected into the data transport network, the user's call may be routed by domain name, IP address or other data for delivery to an associated Web site or other destination. However, this type of hardware provisioning for dial-up service has disadvantages.

[0005]   For one, those consumers who continue to rely upon dial-up connections for access to the Internet and other networks may still desire faster upload and download times, as well as improved overall responsiveness in their browsing experience. Companies deploying PPP dial-up access could, and some commercially may, introduce compression servers or other enhancements in the data path toward that purpose. However, since the transport layer employed is point-to-point, in general the dial-up lines and their associated servers and routers must be dedicated to the individual Internet service providers providing the service. Various telephone numbers for modem access to a provider may for instance all be forced to the same data path.

[0006]   Hardwiring the network edge for specific providers also limits the flexibility of the deployer, owner or operator of that hardware, since no reuse or multiplexing is practical or possible. This among other things makes the cost or amortization of that equipment greater, since it can not be shared among providers or others. Other problems exist.

SUMMARY OF THE INVENTION

[0007]   The invention overcoming these and other problems in the art relates in one regard to a system and method for enhanced data connections via a telephone network, including a front-end facility for receiving modem or other calls over public switched telephone trunks. Modem calls originally configured to request and receive PPP-type connections to a given service provider may be identified by domain name or other identifiers, and injected into a virtual private network or tunnel which connects the call to an enhancement cluster which mediates the user's access to the Internet or other networks. The enhancement cluster may

contain engines to perform compression, caching, optimization, and security and other processing on the user's upstream and downstream data. The data packets may be encapsulated in a higher-level tunneling protocol, so that the transmitted data may still assume that PPP-type transport is being used. In this manner, dial-site owners or operators may allow end users to make use of the asymmetric data network to establish virtual point-to-point connections with providers offering transparent compression, caching, optimization, and security or other enhanced services to end users.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008]   The invention will be described with reference to the accompanying drawings, in which like numbers reference like elements.

[0009]   Fig. 1 illustrates a dial-up access network, according to a conventional embodiment.

[0010]   Fig. 2 illustrates an enhanced dial-up access network, according to an embodiment of the invention.

[0011]   Fig. 3 illustrates a logical diagram of data transport according to a tunneling protocol.

[0012]   Fig. 4 illustrates an example format of a tunneling protocol.

[0013]   Fig. 5 illustrates an enhanced dial-up access network, according to another embodiment of the invention.

[0014]   Fig. 6 illustrates overall connection processing, according to an embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

[0015]   An illustrative environment in which an embodiment of the invention may operate

is shown in Fig. 2, in which a set of end users 102 may communicate over the public switched

telephone network 104 to a set of remote access servers 106. The set of end users may connect

to the public switched telephone network 104 and the set of remote access servers 106 using, for

example, dial-up modems such as modems equipped to perform ITU v.90, v.92 or other

protocols. The set of end users 102 may access the public switched telephone network 104 and

set of remote access servers 106 using, for example, a computer equipped with a Web browser or

other hardware or software and communicating data packets using the Internet Protocol (IP) or

other protocols or standards. The set of remote access servers 106 may be, include or interface

to commercially available RAS platforms such as the Lucent Technologies Inc. APX^{TM} 8000s, or

other hardware, software or other resources. The set of remote access servers may interface to

the public Signaling System 7 network 128 via signaling switch 110, for instance to provide call

setup and call information relevant to the packet switched data network. Upon receipt of an

inbound modem call, the set of remote access servers 106 may likewise communicate with an

authentication server 112 to authenticate the user or account initiating the call, to authorize

access to Web or other service.

[0016]   The set of remote access servers 106 may likewise route traffic to a set of

switches 108. The set of switches 108 may be, include or interface to commercially available

switch hardware such as the Cisco Systems Inc. Catalyst^{TM} 6509, or other hardware, software or

other resources. The set of switches 108 may in turn route traffic to a set of access concentration

routers 114 which coordinate and route traffic to and from the set of end users 102, a group of

enhancement resources described herein, and a destination network 130 such as the Internet or other networks or sites.

[0017]　　　More specifically, the set of remote access servers 106 may receive IP datagrams from the set of end users 102, such as requests to view Web sites, email access, and other data, and communicate that data to concentration routers 114 for routing to processing by an enhancement cluster 118. In embodiments, the set of remote access servers 106 may establish a secure virtual connection or tunnel 116 connecting the set of remote access servers 106, the set of switches 108, the access concentration routers 114 and that enhancement cluster 118.

[0018]　　　In embodiments, the tunnel 116 may be or include a connection established using a tunneling protocol 136 such as the Layer 2 Tunneling Protocol (L2TP), known to persons skilled in the art, and an illustration of whose logical configuration is shown in Fig. 3. Fig. 4 further illustrates a datagram including header generated according to L2TP standards, including fields or flags for type (T, data or control), length (L), sequence (S), offset (O), priority (P), version (Ver), message length (Length), session ID, sequence number for data or control message (Ns), next sequence number (Nr) and offset size (indicating payload start). As shown Figs. 3 and 4, L2TP as an operative tunneling protocol 136 may encapsulate IP, PPP or other data in a higher-lever datagram intended for delivery via virtual or other networks or connections. Those objects may be formatted to L2TP standards as promulgated by the Internet Engineering Task Force (IETF), or according to other formats or standards known by persons skilled in the art. According to the invention in another regard, the tunnel 116 may employ security features such as the IP Security (IPsec) protocol, and establish or include connections via the Universal Datagram Protocol (UDP) or other formats or channels.

[0019]   According to the invention in one regard, therefore, users among the set of end users 102 may initiate a dial-up session to the set of remote access servers 106, using a browser and IP connections, or other clients and connection configurations, and directed through tunnel 116 using tunneling protocol 136.

[0020]   In general, unenhanced IP communications send data packets into the network on a connectionless basis, so that datagrams traverse any available route to the destination, based for instance on least-latency or other rules. However, according to the invention in one regard the user may dial in to the set of remote access servers 106, for instance a private Internet provider dial site, which may sense the call as being designated for enhanced service and direct the transport to PPP-compatible links. For example, the authentication servers 112 may detect an enhanced call through the use of a special domain name or extension. That domain name or extension may for example take the form "Enhanced.Sprint.com" or other. The set of authentication servers 112 may interpret that target domain as a request to access enhanced throughput, storage or other services. In embodiments, the dialer, browser or other client or other software being used by the user may attempt to establish a PPP session to directly connect to the desired Web site.

[0021]   However, according to the invention that modem call may be directed by the set of remote access servers 106 to tunnel 116 and ultimately to the enhancement cluster 118, based on the destination address or other identifier. The enhancement cluster 118 may perform compression, concentration, caching, optimization, and security and other functions on the user's data stream. Enhancement cluster 118 may likewise connect the user's session to or via the Internet using the underlying IP or other protocols. Since the user's data packets travel on a directed route through tunnel 116 from the set of remote access servers 106, set of switches 108,

set of access concentration routers 114 and to enhancement cluster 118, that cluster may apply bidirectional compression/decompression, caching or other enhancements to the Internet or other session, resulting in a more responsive feel to the user. In general, the compression or other enhancement should or must occur in the data path so that enhancement can be performed on both upstream and downstream data flows.

[0022]   In embodiments, the user's data packet, which may have originated in PPP or other format, may traverse the tunnel 116 assuming that the connection to enhancement cluster 118 is direct, when in fact the connection may be indirect or otherwise. However, because the user's data stream is spoofed or made to believe or behave as though it were direct, the non-symmetric, hybrid telephone/computer network along which traffic is flowing may convey data types which assume a symmetric connection, such as PPP or other protocols. Thus, access to enhanced Web sites and other destinations may be provided to any number of users, discriminated on destination domains and without the necessity for dedicated trunks to service the point-to-point traffic of individual providers.

[0023]   When data from the user's session arrives at the enhancement cluster 118, that data may be routed and processed to perform a variety of enhancements may be performed on that data. As illustrated in Fig. 2, the traffic may be communicated via tunnel 116 to the enhancement cluster 118 and received in a set of load balancers 124 which distribute data within enhancement cluster 118. The set of load balancers 124 may communicate the user's data stream to a set of compression servers 126. The set of compression servers 126 may compress the data stream, for instance using software, hardware or other compression techniques, for example at ratios of up to 5:1 or more depending on factors such as compression type and the data being subjected to compression.

[0024]   The set of compression servers 126 may also perform other or further processing, such as the caching of a user's frequented pages or other locations for faster access. The set of compression servers 126 may perform other services or enhancements as well, such as encryption or other security or other processing. Individual users may have different types of enhancement applied to their sessions or accounts, depending for instance on user selection, user subscription type or level, or other factors.

[0025]   Once the set of compression servers 126 have processed the arriving or departing data stream, that data may be communicated back to the set of load balancers 124, and then to a set of cluster switches 120. The traffic switched by the set of cluster switches 120 may then be communicated to the set of access concentration routers 114, which may route the session to the destination network 130 such as the Internet or other network, for instance based on an IP address or other addressing scheme. Data flowing back from destination network 130 may traverse the set of access concentration routers 114 and be routed to the enhancement cluster 118, where compression, caching, optimization, and security or other services may be applied before the data returns via tunnel 116 to the user in the set of users 102 conducting the session.

[0026]   Fig. 5 illustrates an embodiment of the invention, in which incoming modem calls from the set of users likewise terminate in the set of remote access servers 106 for Internet or other access. In the illustrated embodiment, compression, caching, security and other features are however delivered by a set of distributed enhancement platforms 134 via set of tunnels 132, which platforms may be logically or physically separated from each other or other parts of the network. For example, according to embodiments of this type in one regard, various ones or more of the set of distributed enhancement platforms 134 may be hosted by or located at different physical locations, such as on the premises of individual Internet service providers.

Different ones of more of distributed enhancement platforms 134 may supply different types of data stream enhancements, depending on the provider or the user's account or subscription.

[0027] Overall connection processing according to an embodiment of the invention is illustrated in Fig. 6. In step 602, processing begins. In step 604, a user among the set of end users 102 or otherwise may place a point-to-point call to an IP dial site, such as a modem call via the public switched telephone network 104 to a telephone number assigned to an Internet service provider. In step 606, the call may be terminated at the set of remote access servers 106 or otherwise. In step 608, the domain name, password or other information supplied by the end user may be authenticated via authentication server 112. In step 610, the set of remote access servers 106 may generate a tunnel 116 to the enhancement cluster 118 after authentication by authentication server 112, such as for example a L2TP or other tunnel or connection.

[0028] In step 612, the tunnel 116 may be terminated at the enhancement cluster 118, for instance at the set of tunnel servers 122, such as L2TP Network Servers (LNS) or other platforms. In step 614, a temporary IP address may be assigned to the ongoing call for routing to the Internet or other destination. In step 616, the call or session may be routed to one of the set of load balancers 124. In step 618, the call may be routed to one of the set of compression servers 126. In step 620, the one of the compression servers 126 may perform compression, caching, encryption or other security or other processing on the data stream of the call.

[0029] In step 622, the call may be forwarded back to one of the set of load balancers 124. In step 624, the one of the set of load balancers 124 may perform a secured network address translation (NAT) and attach or substitute a unique IP address to the call. In step 626, the call may be routed via the set of access concentration routers 114 to destination network 130 or other destination. In step 628, the Web site or other destination may return data to the end

user via enhancement cluster 118 and tunnel 116, performing for instance corresponding decryption, caching or other processing on the return data stream. In step 630, processing may end, repeat, or return to a prior point.

[0030]   The foregoing description of the invention is illustrative, and modifications in configuration and implementation will occur to persons skilled in the art. For instance, while the invention has generally been described in terms of channeling inbound modem calls to one or more enhancement clusters via the exemplary L2TP protocol as one tunnel protocol 136, other protocols or channels, such as Layer 3 Tunneling Protocol (L3TP), or other certificate-based or other standards-based or proprietary connections may be used. Similarly while the invention has generally been illustrated in terms of the set of end users 102 being or including consumers accessing Internet service providers, other users and other providers may employ platforms according to the invention, such as corporate, government or other employees accessing private networks, storage or other resources via an authenticated tunnel connection.

[0031]   For further example, while the invention has in embodiments been illustratively described as discriminating or directing end users to the enhancement cluster based on the destination domain name, in embodiments other criteria or mechanisms, such as explicit passwords, certificates, cookies or other techniques to identify enhanced service sessions, may be used. The scope of the invention is accordingly intended to be limited only by the following claims.